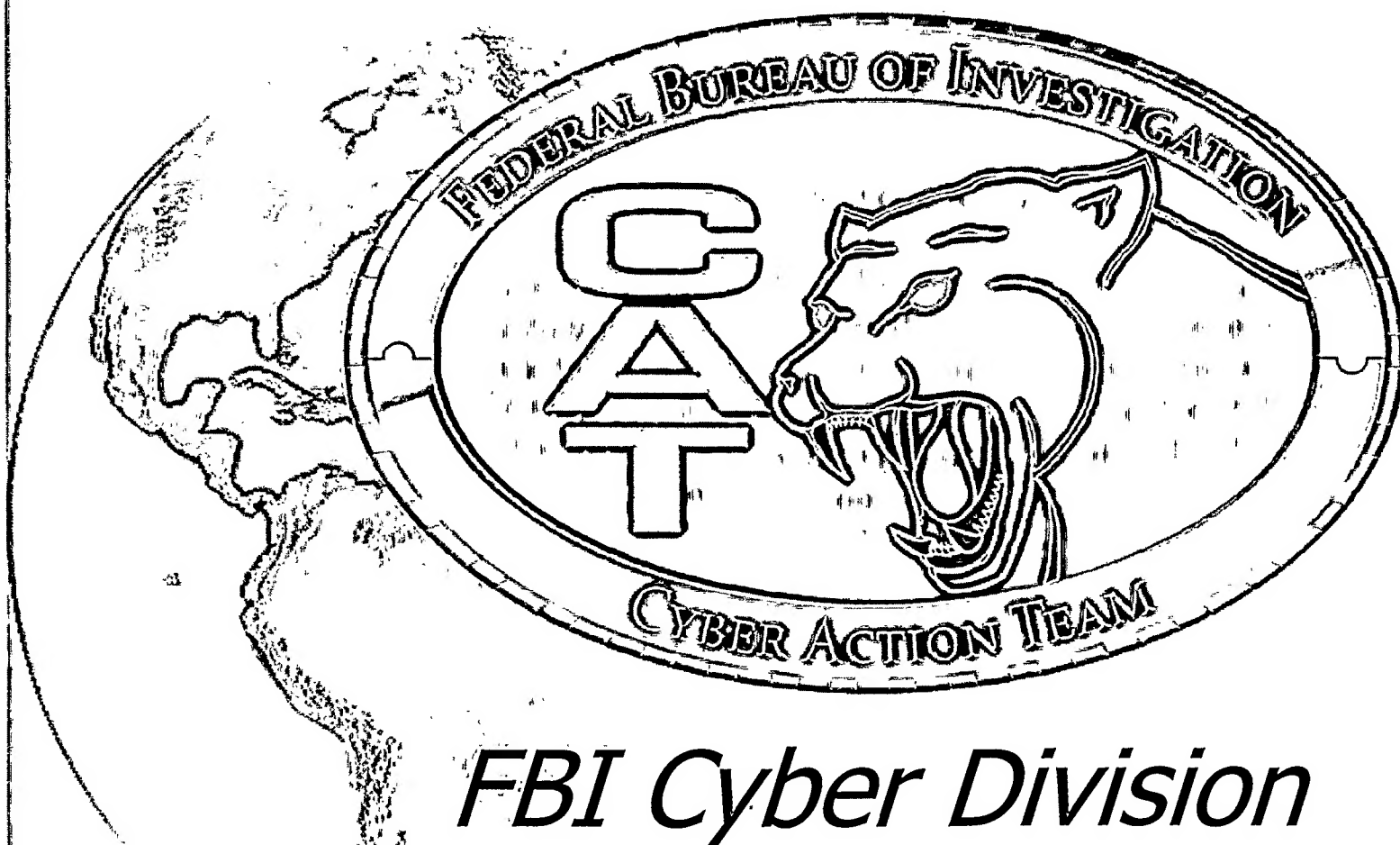


FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1437333-0

Total Deleted Page(s) = 1  
Page 23 ~ b7E;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX



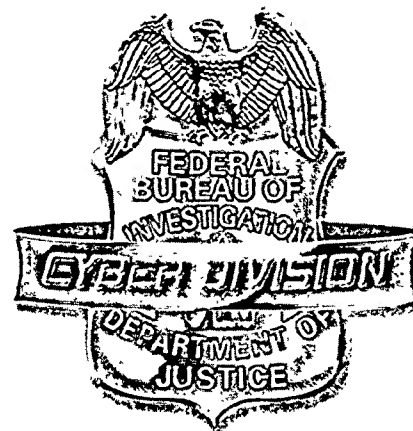
*FBI Cyber Division  
Operation BOT ROAST*





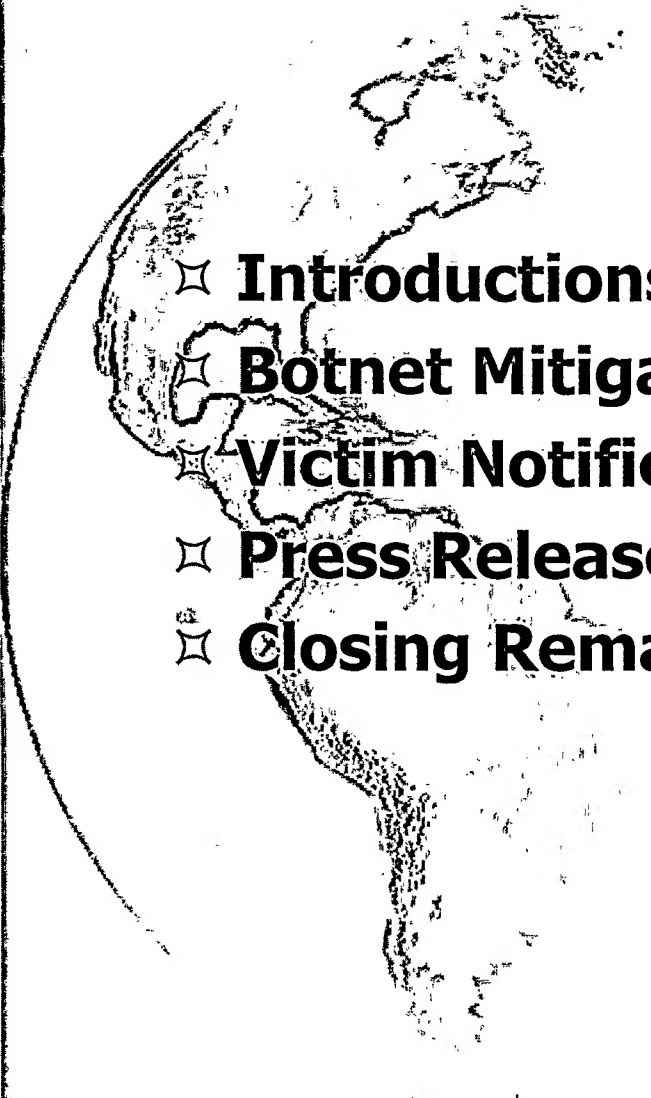
# ***Operation BOT ROAST***

***Botnet Initiative National Takedown***



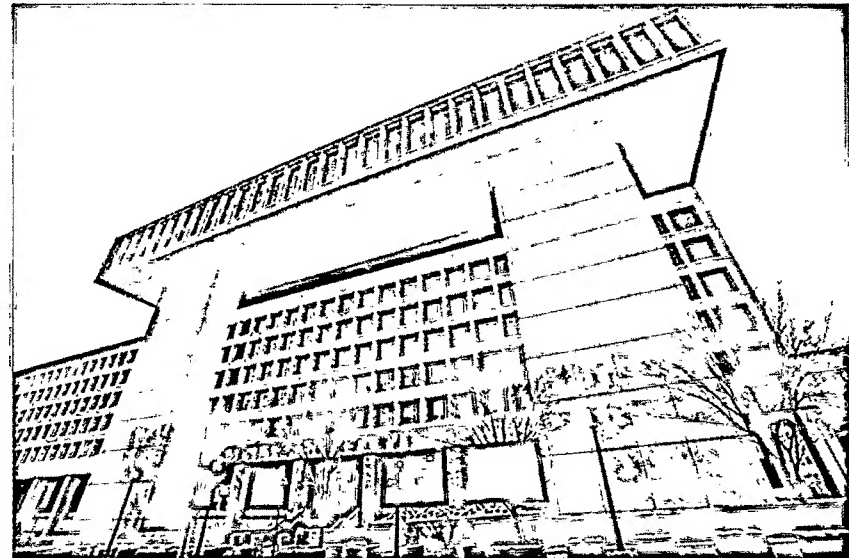
*July 12, 2007*  
*BOTCON 6*  
*Sydney, Australia*

# *Agenda*

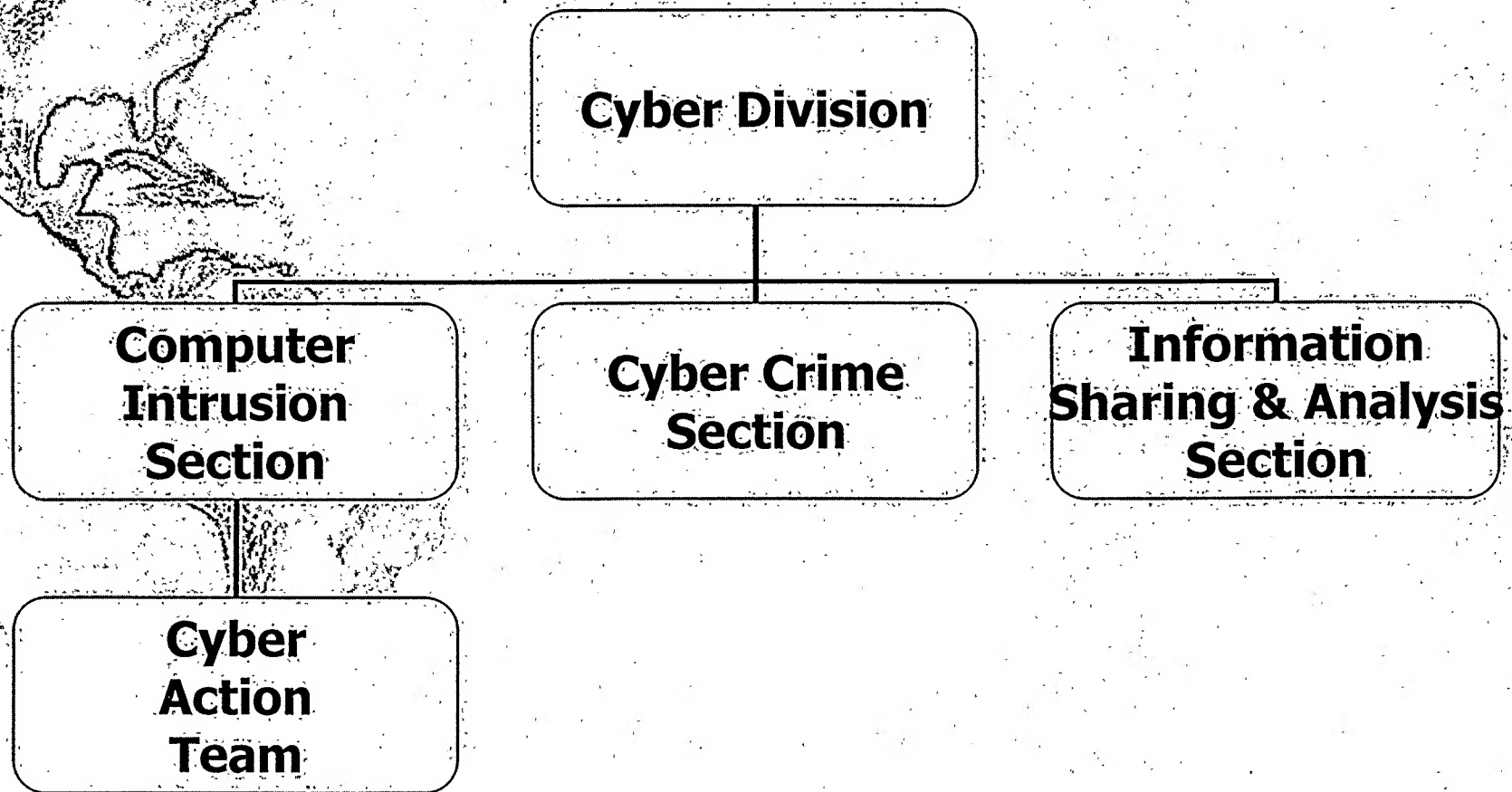
- 
- ✧ **Introductions**
  - ✧ **Botnet Mitigation Strategy**
  - ✧ **Victim Notification Strategy**
  - ✧ **Press Release/Media Strategy**
  - ✧ **Closing Remarks**

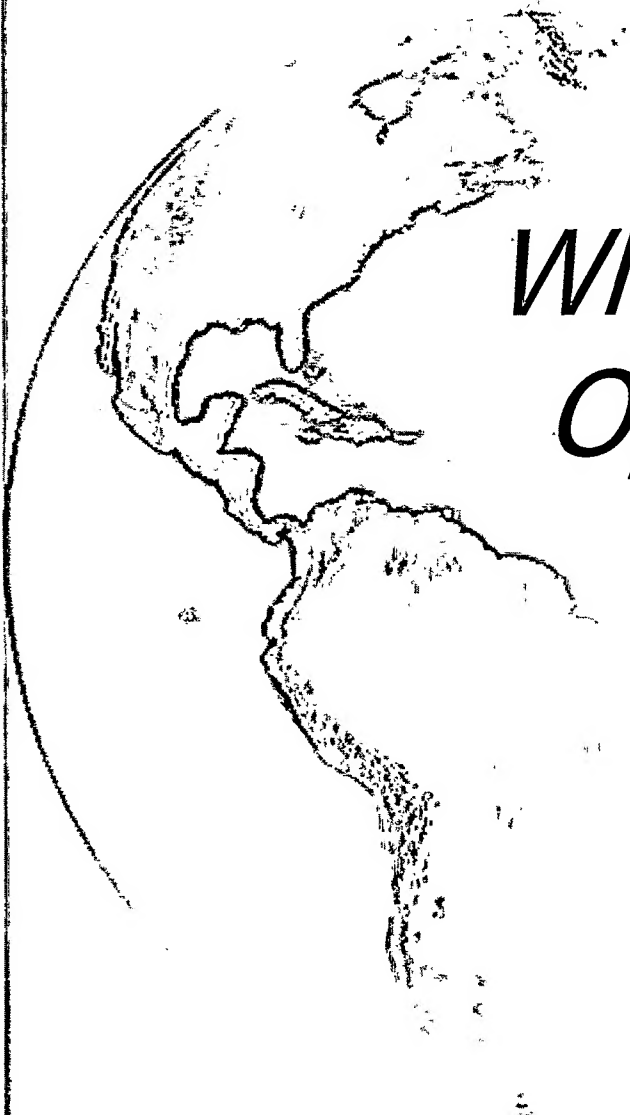
# *Introduction-*

- ✧ **Supervisor at  
FBIHQ Cyber  
Division**
- ✧ **Philadelphia Div**
- ✧ **8 Years**
- ✧ **FBI National  
Botnet  
Coordinator**



# *FBI Cyber Division*





*What was the genesis of  
Operation BOT ROAST?*

*Answer: Botnet Task Force*

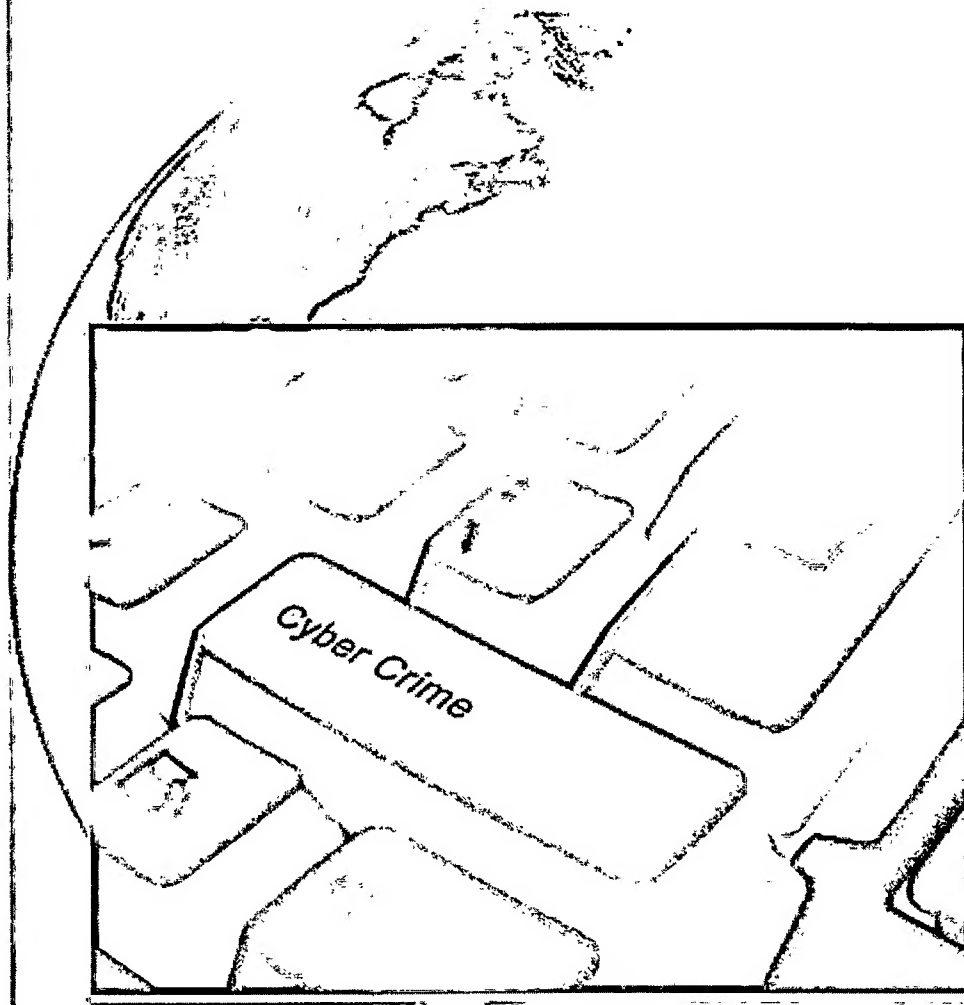
*October 2006*



- ✧ **Botnet Task Force discusses plans for a coordinated takedown**
- ✧ **Multi-National takedown**
- ✧ **Extremely difficult**



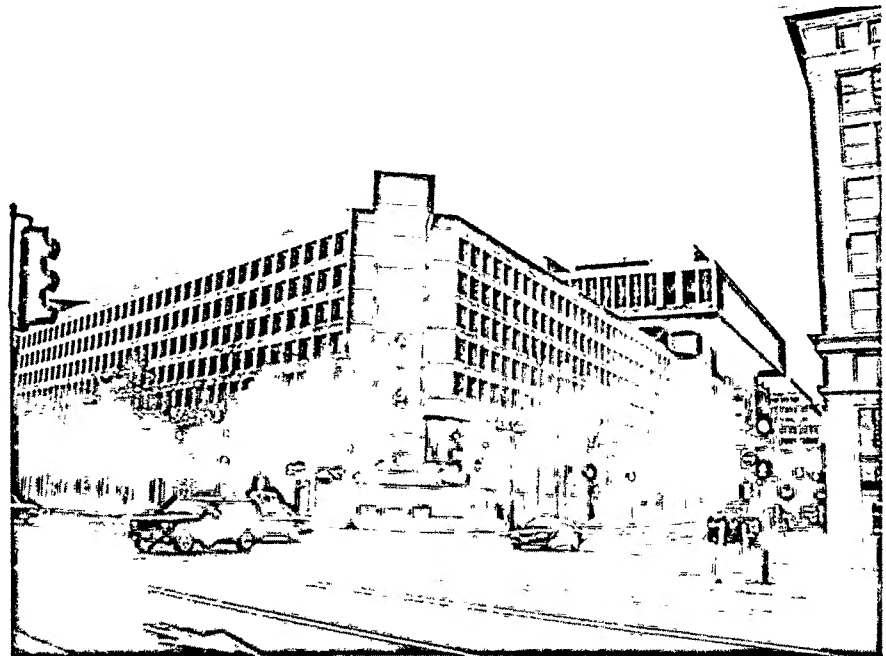
*March 2007*



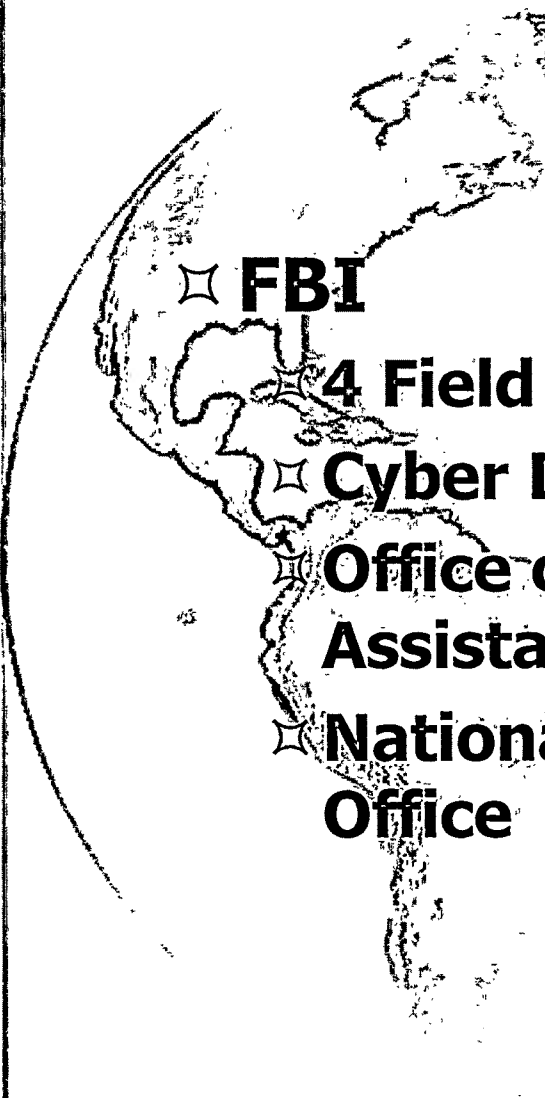
- ✧ **FBI Cyber Division initiates National Botnet Takedown Operation**
- ✧ **Operation BOT ROAST**
- ✧ **Operation is small in nature, approximately four (4) field offices**

# *Operation BOT ROAST : Goals*

- ✧ **Botnet Mitigation Campaign**
- ✧ **Public Awareness Campaign**
- ✧ **Victim Notification Campaign**
- ✧ **Media and Press Campaign**



# *Operation BOT ROAST: Players*



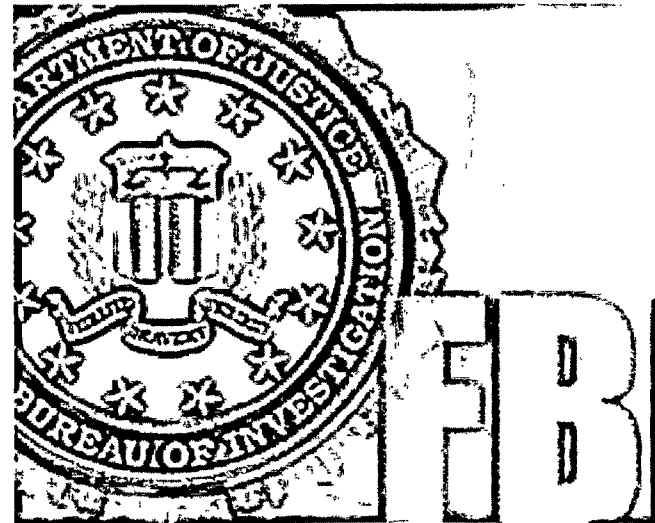
✧ **FBI**

✧ **4 Field Offices**

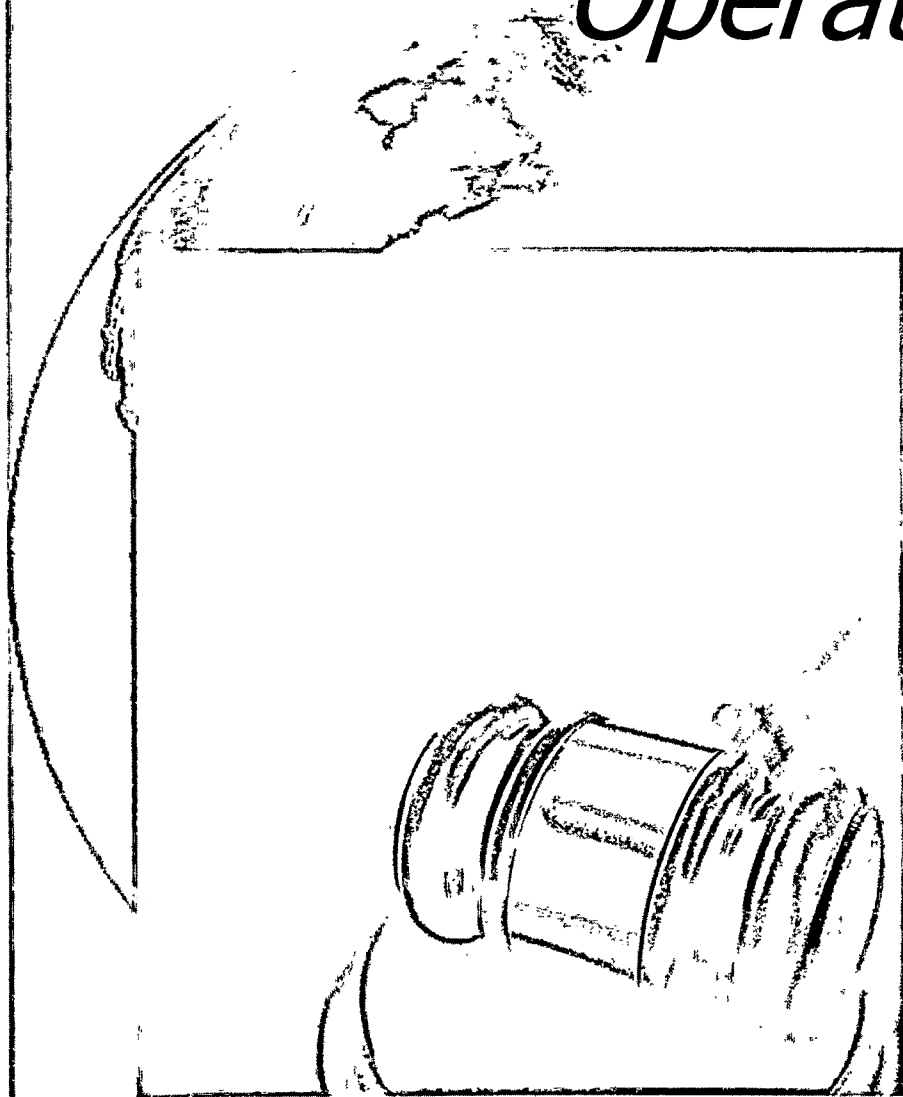
✧ **Cyber Division**

✧ **Office of Victim  
Assistance**

✧ **National Press  
Office**



# *Operation BOT ROAST: Players*



## ✧ **FBI**

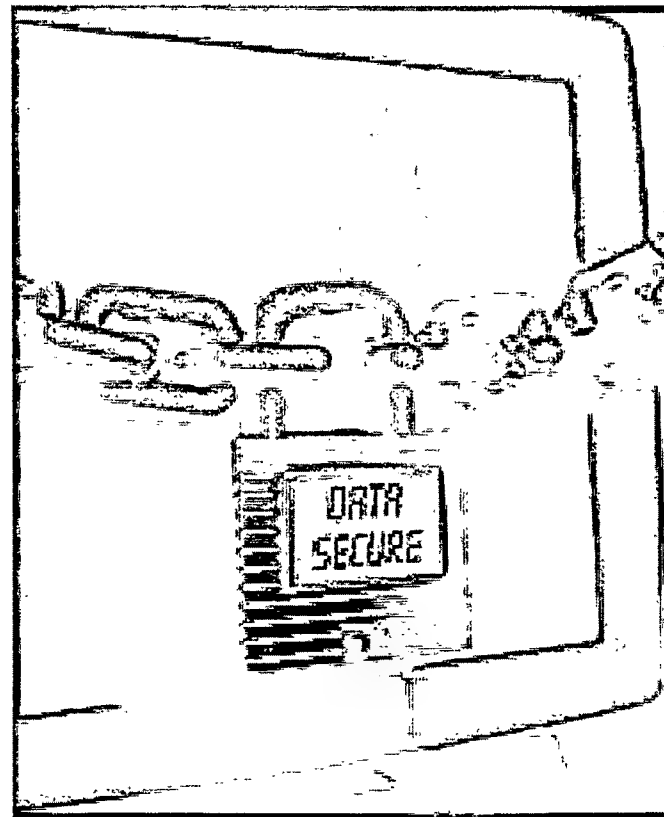
- ✧ **CART- Forensics**
- ✧ **General Counsel**
- ✧ **Internet Crime  
Complaint Center**

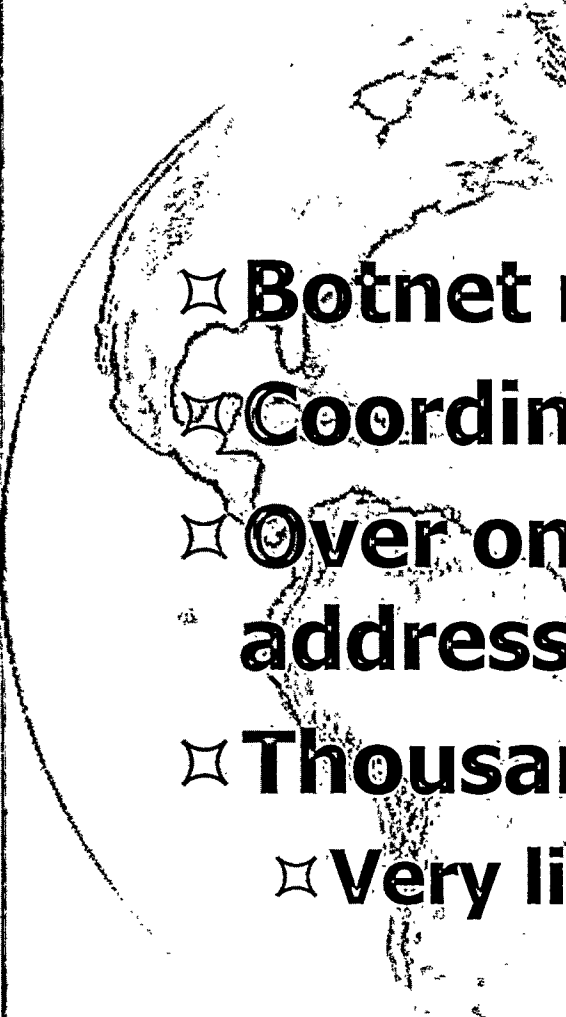
## ✧ **US Department of Justice**

- ✧ **Computer Crimes  
& Intellectual  
Property**

# *Operation BOT ROAST:* *Players*

- ✧ **Internet Service Providers**
- ✧ **Microsoft**
- ✧ **CERT  
Coordination  
Center**
- ✧ **US CERT**

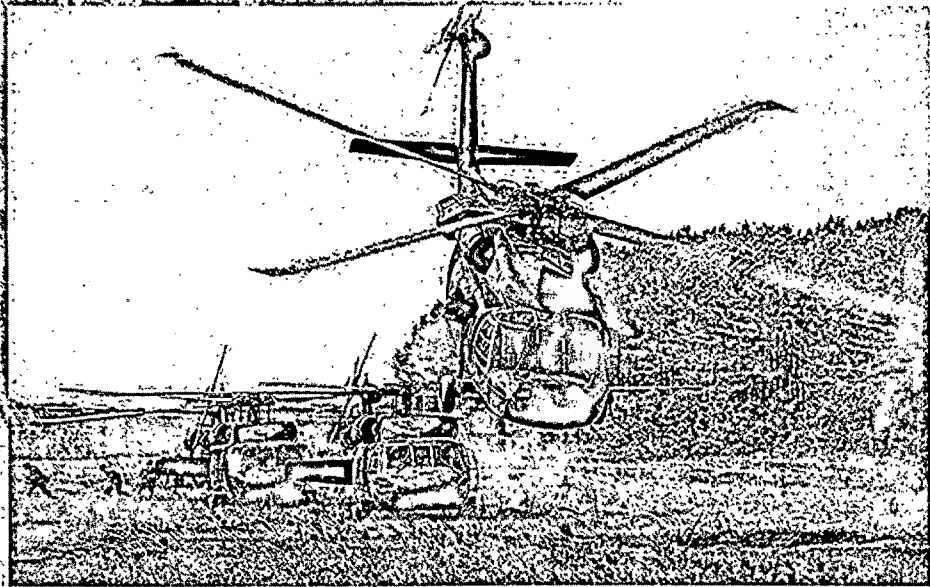




# *Operation BOT ROAST: Battlefield*

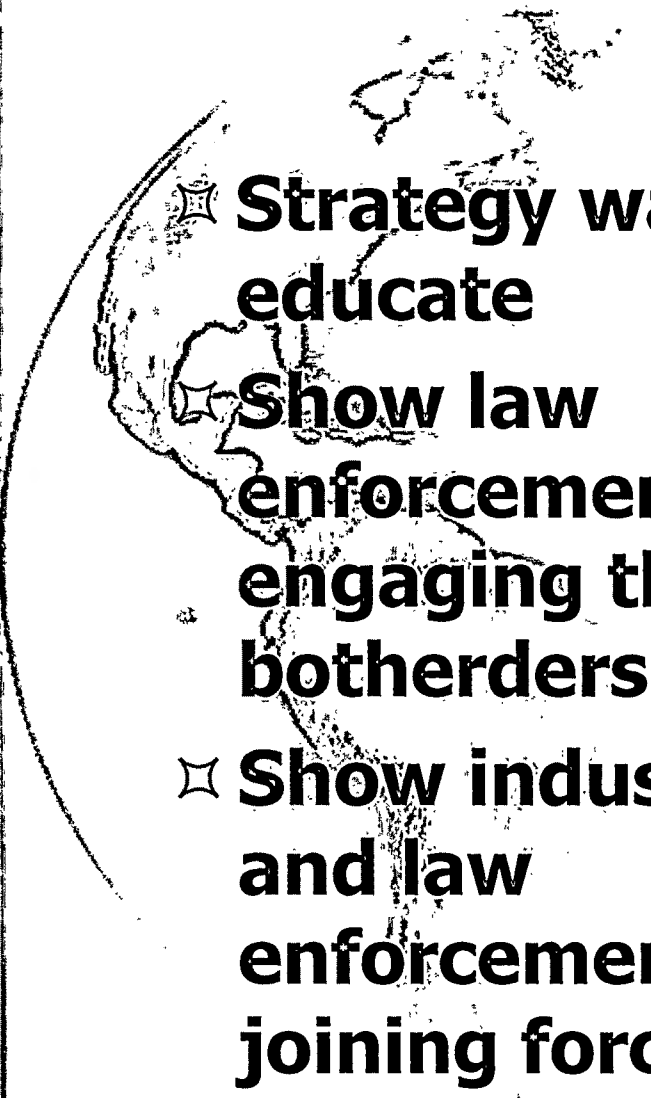
- ✧ **Botnet mitigation = Difficult**
- ✧ **Coordination = Challenging**
- ✧ **Over one million victim IP addresses**
- ✧ **Thousands of fraud malware**
  - ✧ **Very little botnet C&C malware**

# *Operation BOT ROAST Strategy*



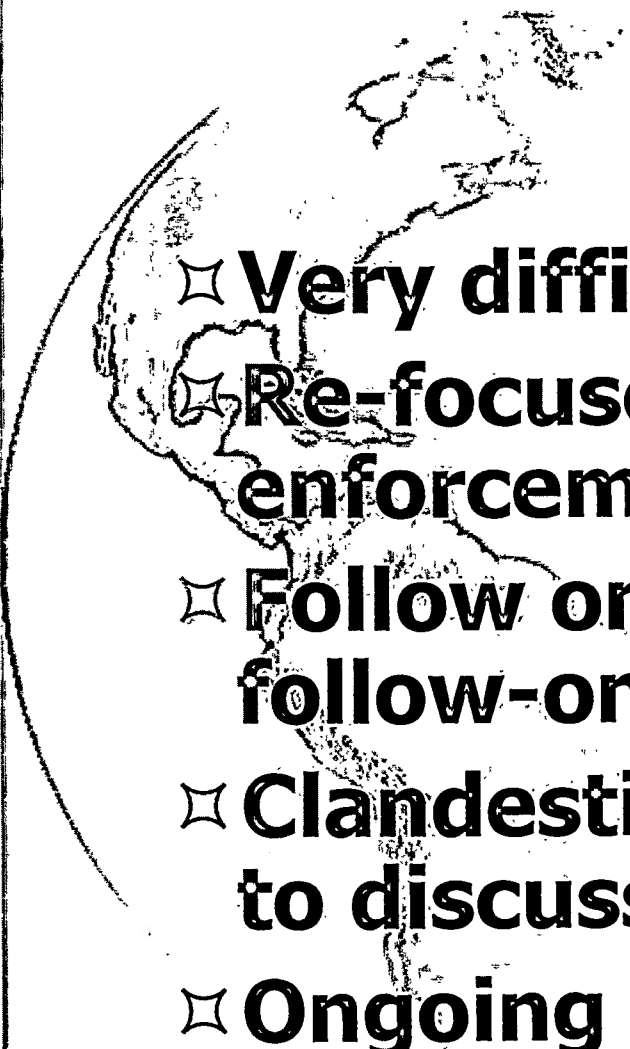
- ✧ **Public Awareness Campaign**
- ✧ **To disrupt and deter the Botnet Underground**
- ✧ **To disrupt and deter online criminals utilizing botnets**

# *Public Awareness*

- 
- ✧ **Strategy was to educate**
  - ✧ **Show law enforcement is engaging the borderers**
  - ✧ **Show industry and law enforcement are joining forces**

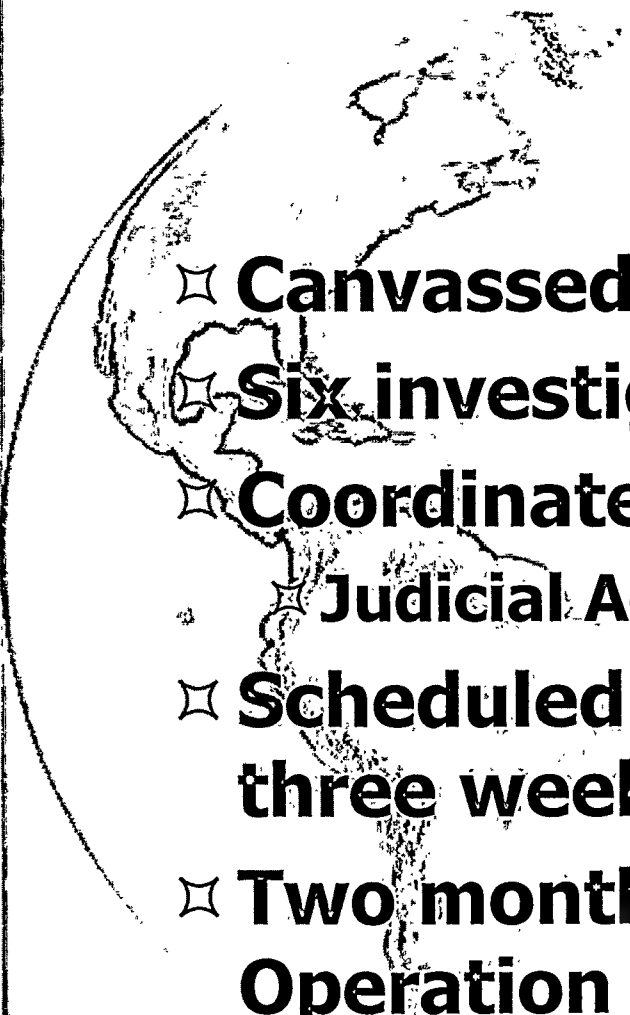






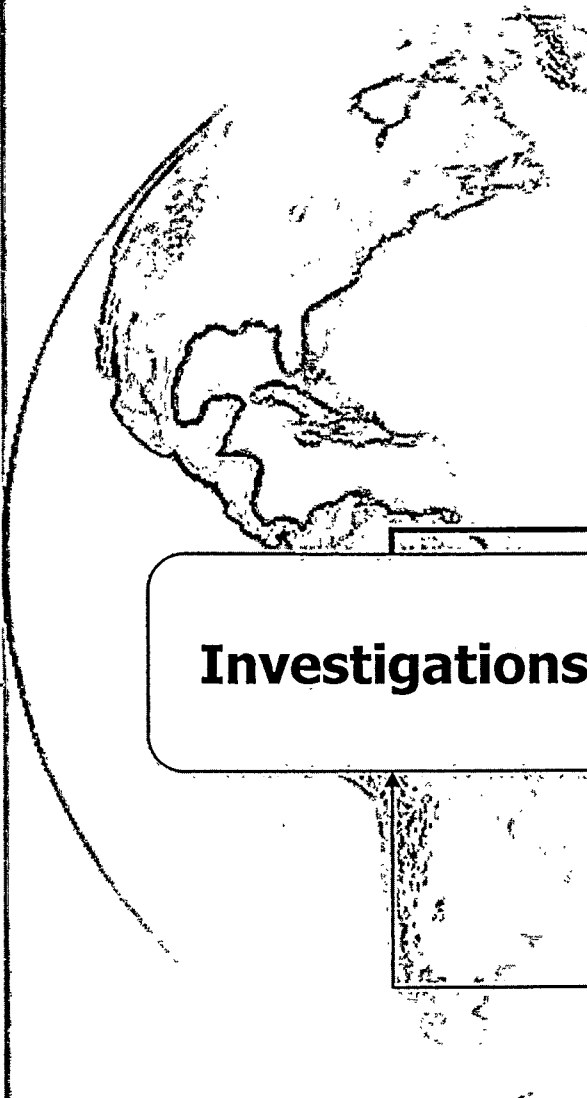
## *Operation BOT ROAST: Mitigation*

- ✧ **Very difficult task**
- ✧ **Re-focused on botnet crimes law enforcement could prosecute**
- ✧ **Follow on botnet activity through follow-on investigations**
- ✧ **Clandestine meeting with industry to discuss strategy**
- ✧ **Ongoing Operation**

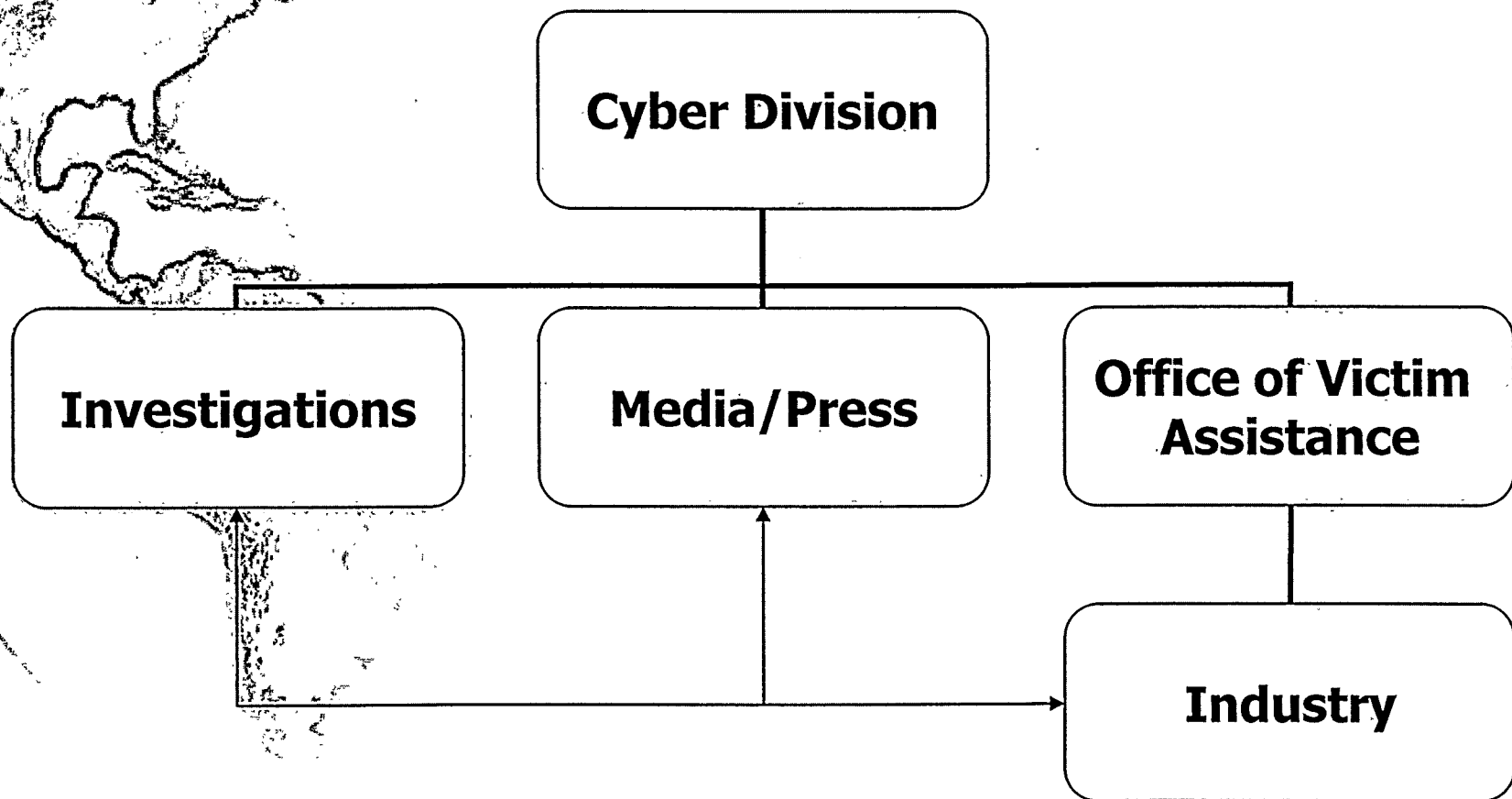


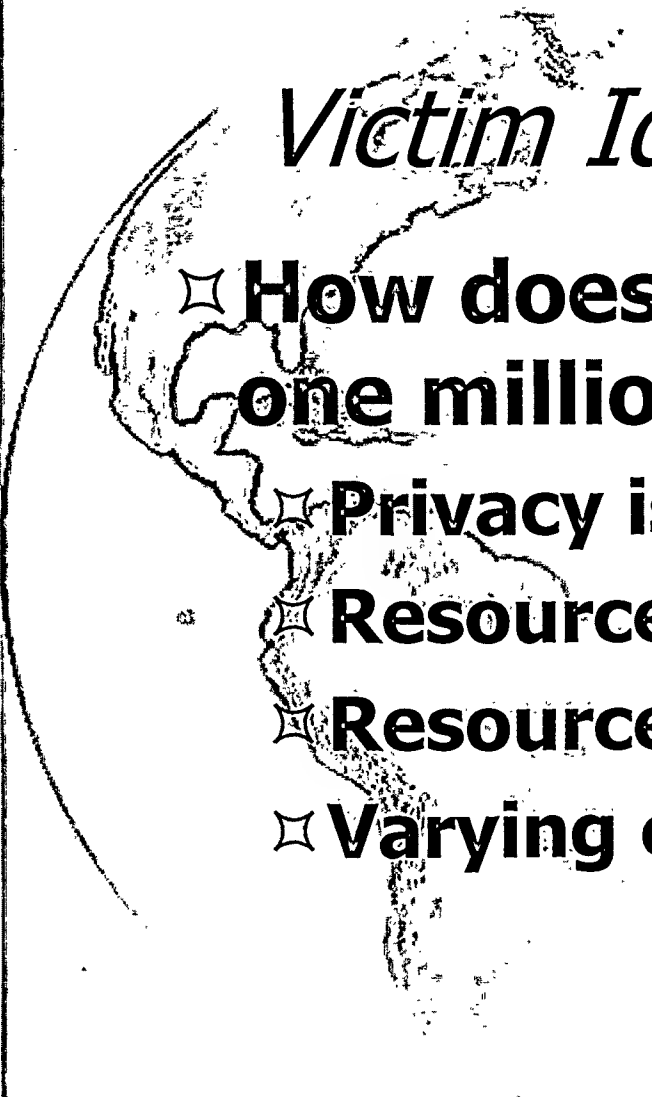
## *Operation BOT ROAST: Coordination*

- ✧ **Canvassed investigations**
- ✧ **Six investigations identified**
- ✧ **Coordinated takedown**
- ✧ **Judicial Action on or about the same time**
- ✧ **Scheduled conference calls appx every three weeks.**
- ✧ **Two months scheduled to execute Operation BOT ROAST**



# Investigations





## *Operation BOT ROAST: Victim Identification Notification*

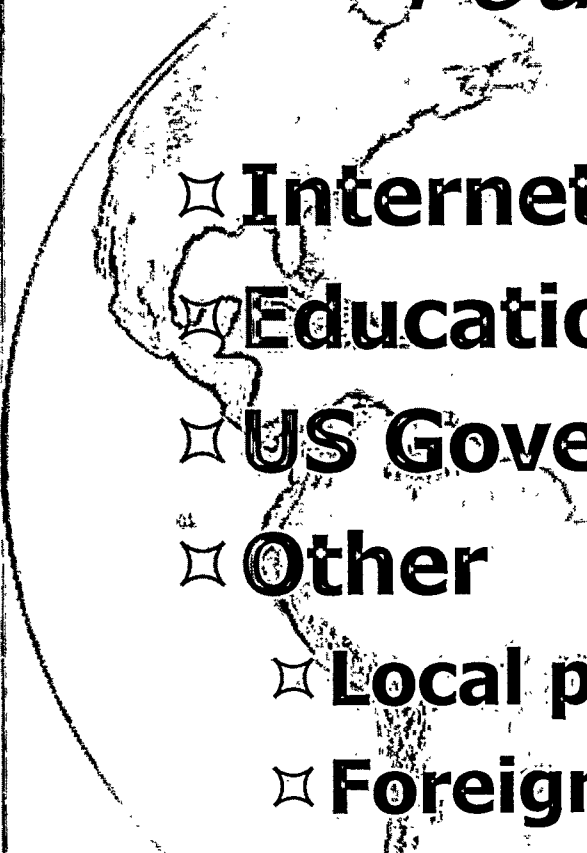
✧ **How does one identify and notify  
one million victim IP addresses?**

✧ **Privacy issues**

✧ **Resources to identify**

✧ **Resources to notify**

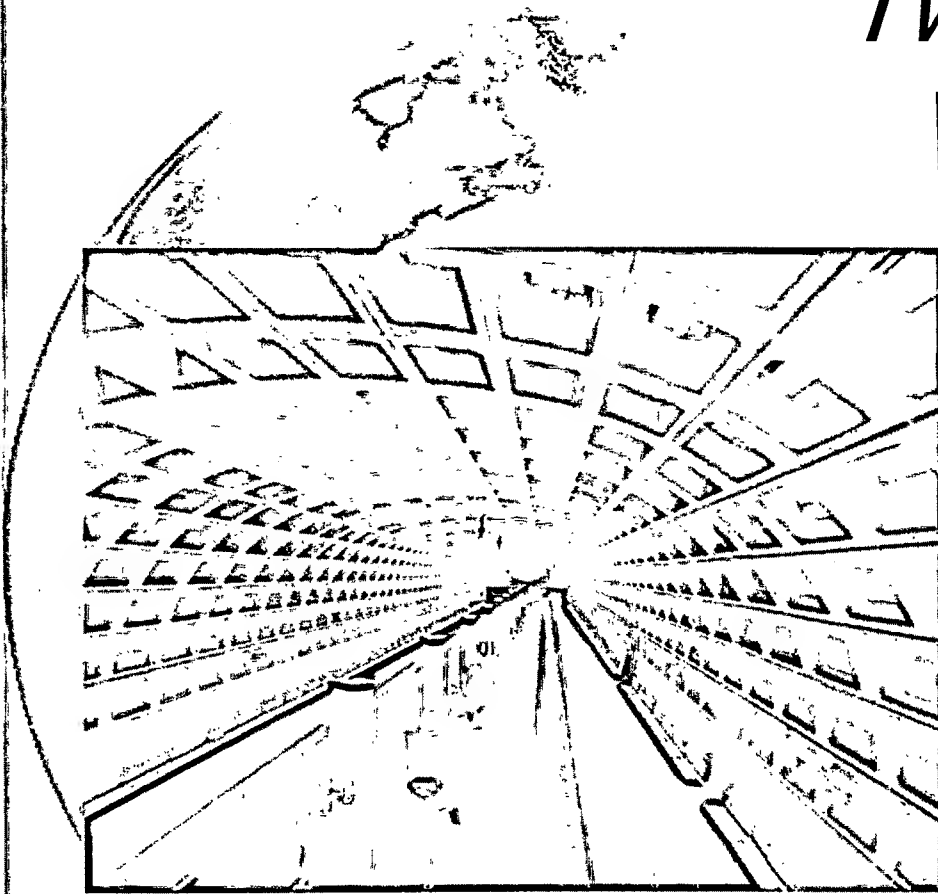
✧ **Varying categories of victims**



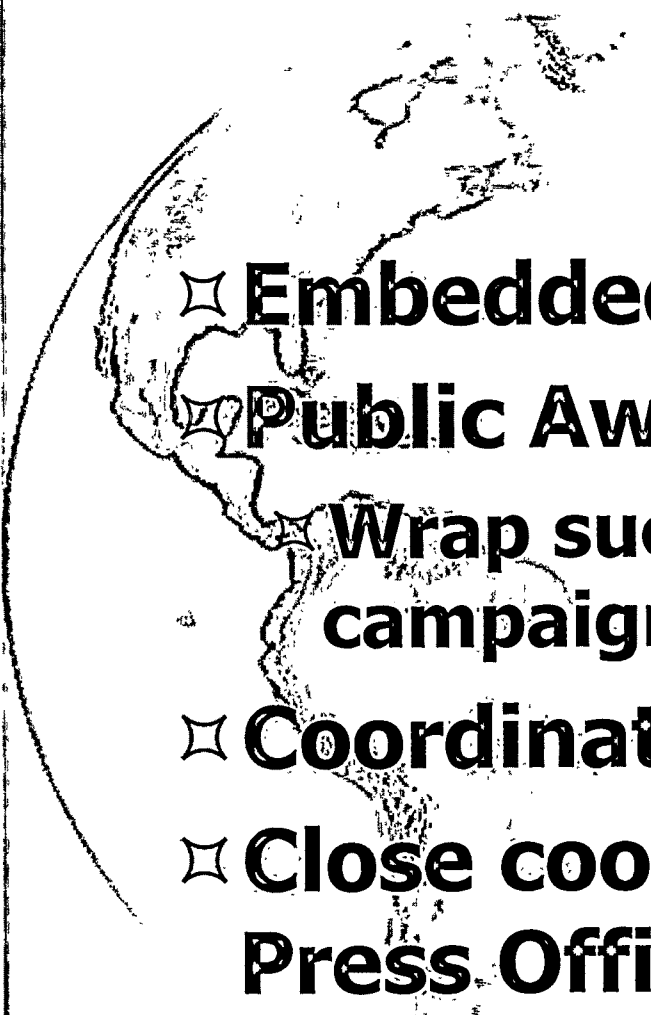
## *Four Categories of Victims*

- ✧ **Internet Services Providers**
- ✧ **Education Institutions**
- ✧ **US Government (US CERT)**
- ✧ **Other**
  - ✧ **Local providers**
  - ✧ **Foreign Government**
  - ✧ **Foreign ISP**

# *Two Wave Process: Victim Notification*



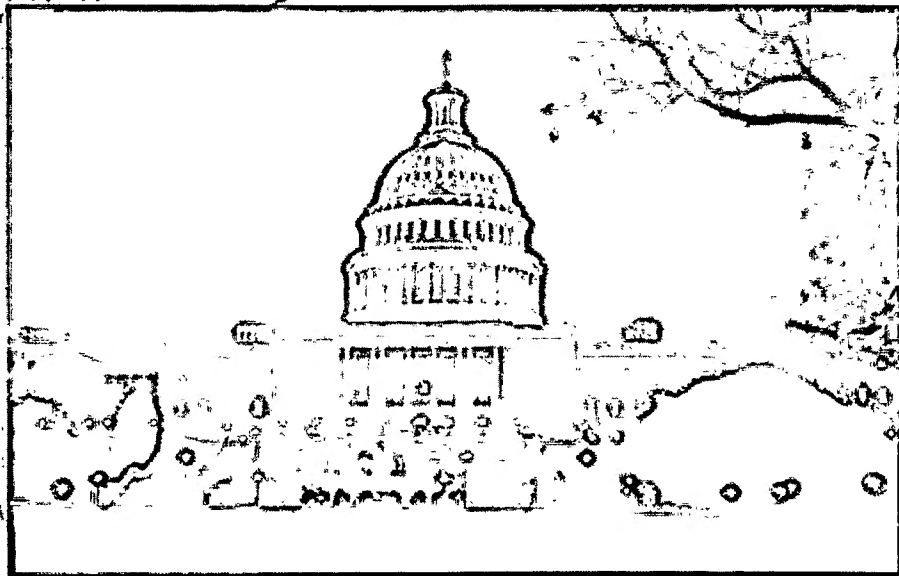
- ✧ **First Wave:**
  - ✧ **Provide IP addresses to potential victims**
- ✧ **Organization confirms it's a victim**
- ✧ **Second Wave:**
  - ✧ **Provide victim assistance**



# *Press/Media Strategy*

- ✧ **Embedded reporters**
- ✧ **Public Awareness emphasis**
- ✧ **Wrap successful cases around the campaign**
- ✧ **Coordination with Industry**
- ✧ **Close coordination with National Press Office**

# *Operation BOT ROAST: Ongoing Operations*

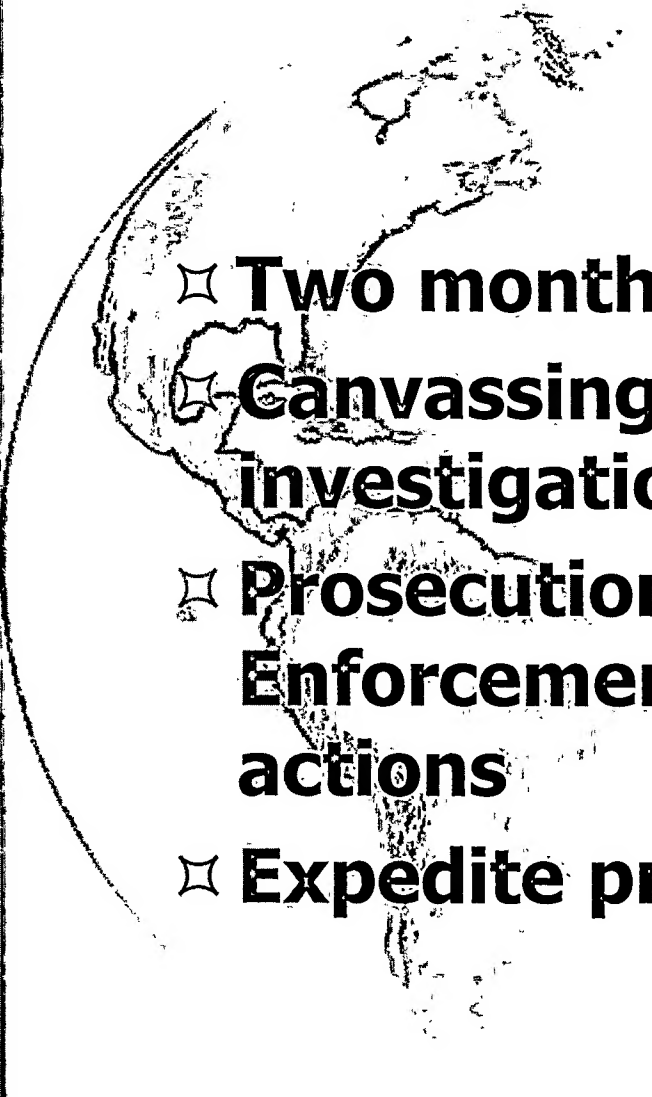


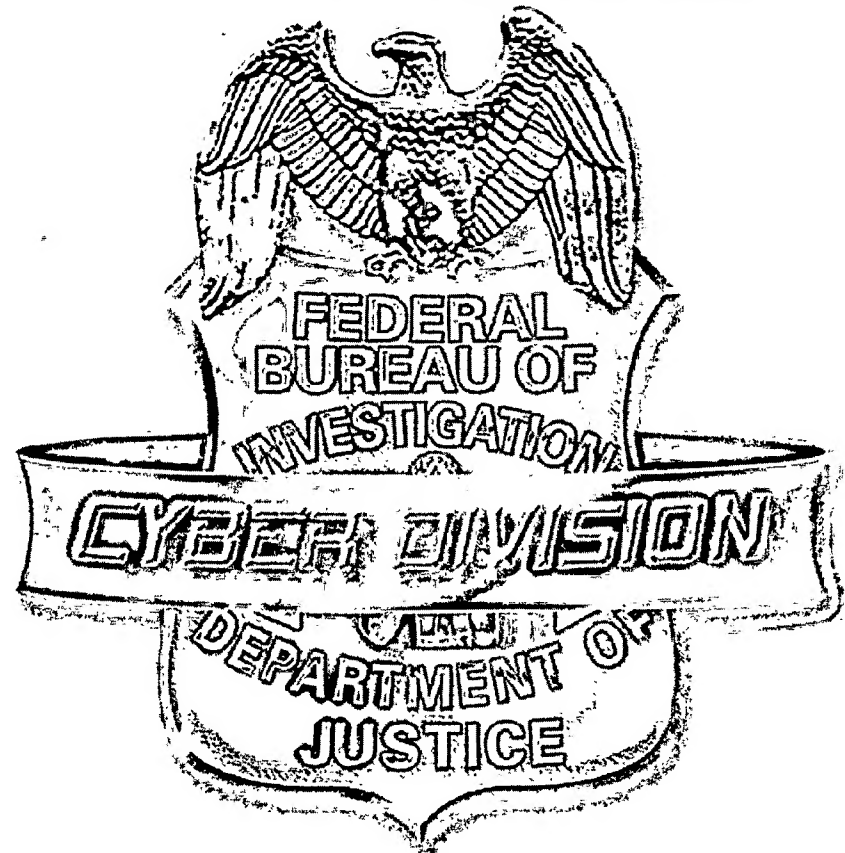
## ✧ **Continuing:**

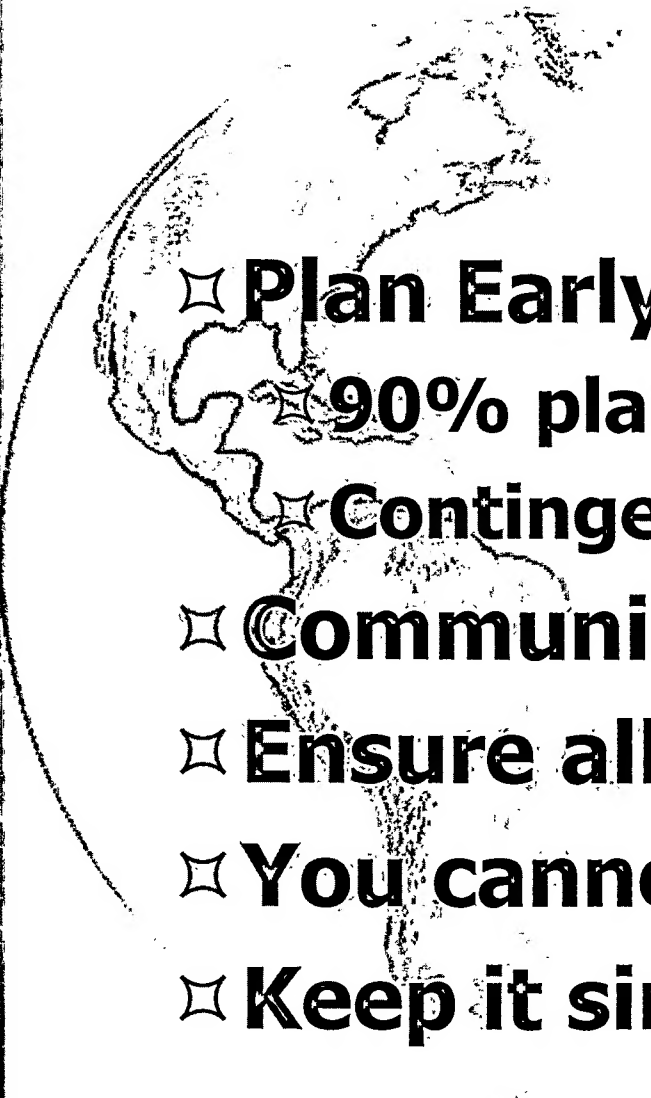
- ✧ **Victim Notification**
- ✧ **Malware Analysis**
- ✧ **Data  
Dissemination**
- ✧ **Investigations**
- ✧ **Prosecution**



# *Operation BOT ROAST: Round II*

- 
- ✧ **Two months**
  - ✧ **Canvassing investigations**
  - ✧ **Prosecution, Law Enforcement actions**
  - ✧ **Expedite process**





# *LESSONS LEARNED*

- ✧ **Plan Early, Plan Often**

- ✧ **90% planning, 10% Execution**

- ✧ **Contingency plans**

- ✧ **Communicate clearly with brevity**

- ✧ **Ensure all parties are participating**

- ✧ **You cannot please everyone**

- ✧ **Keep it simple**



*Operation*  
**BOT ROAST:**  
*Questions?*

